CNS-105-2 Critique #5

徐彥旻 b03901027

Laurent Eschenauer and Virgil D. Gligor. "A key-management scheme for distributed sensor networks," in ACM conference on Computer and communications security, 2002.

Summary

1. *introduction*
   比較 Distributed Sensor Networks(DSNs) 與 traditional embedded wireless networks ，指出 DSNs 規模較大且是動態的。討論了通訊安全與金鑰管理在實作上的限制，以及之前的人提出的方法為何不適用。
2. *basic scheme*
   a. 金鑰分配分為三個階段：1)對於每個 sensor，從固定數量的金鑰中隨機選取不重複的 k 個金鑰，預先放在 sensor 當中，2)有共同的金鑰的 node 彼此建立連結，3)對於沒有直接的連結的點，尋找連結的路徑。
   b. 當有 node 被攻佔，對應的 controller 會廣播對應的 node 的金鑰，每個 node 廢棄這些金鑰，重新建立連結的路徑。
   c. 當 node 上的金鑰使用時間過長，會自己廢棄這些金鑰。
   d. 當有 node 被攻佔，相較於其他方案，本篇提出的金鑰管理受到影響的 node 數量比較少。
3. *analysis*
   a. 從隨機圖形的推論，可以得知為了讓圖形連在一起所需的連結數期望值，以及給定 node 數量 n 、單一 node 能有的金鑰數 k 後，金鑰總數 P 該如何選取。
   b. 當可單一 node 可以連結的 node 數量變為 $n\prime<<n$ ，若要保有相同的連結數期望值，則需要大幅增加 k 。
4. *simulations*
   用模擬驗證以上的推論。

Strengths

- 對於攻擊方的假設合理，應用隨機圖形的數學分析以及模擬，改進了前人的缺點。
- 提出的方法能夠在某些 node 遭受攻佔後，於可接受的成本內回復安全運作。

Weaknesses

如果 sensor 的記憶體真的太小，無法存放足夠數量的金鑰的話，要另外做處理才行。

CNS-105-2 Critique #5

Reflection

- 將問題抽象化，套用既有的數學推論，是研究的突破方式之一。
- 這篇論文被引用次數在 google scholar 上顯示為 4358 次，至少可以說是在學術界有被熱烈討論的，或許是跟物聯網的趨勢有關。